Amendments to the Specification

Please replace the second paragraph beginning on page no. 2 with the following paragraph:

Data transmission networks are extremely well known and used throughout the prior art. ~~Networks~~ **Network** characteristics which differentiate one network from another include: topology or the geometric arrangement of connection devices to the transmission medium; the data transmission technology used for data transfer (transmission protocols are the specification standards for sending types of data); and the substance used for the propagation of signals, *i.e.*, the transmission media. The most common topology or general configurations of networks include the bus, star, and Token Ring topologies. Information networks can also be characterized in terms of spatial distance as local area networks (LAN), metropolitan area networks (MAN), and wide area networks (WAN). For simplicity, the discussion herein will categorize exemplary networks by the substance used for the propagation of signals, *i.e.*, the transmission medium, because, as a practical matter, the threshold inquiry for an enterprise network frequently centers around the transmission media. Such ~~substance~~ medium substances include copper, *e.g.*, twisted-wire pair, coaxial cable and power, fiber-optic cable, air, dielectric-slab waveguide, and even water. For the purposes herein, only copper, fiber-optic cable and air transmission mediums need be discussed.

Please replace the first paragraph beginning on page no. 4 with the following paragraph:

With the exception of CCTV, each of the above identified types of distribution systems are dependent on a broadband transmission medium, while LANs may be successfully operated over a less expensive twisted pair media. As a practical matter, while LAN components were once widely available with BNC connectors (British Nautical Connectors), presently [[,]] virtually all LAN network components are ported with RJ-45 eight conductor twisted pair connections. CCTV distribution systems, which

are largely relegated to surveillance systems, are a mix of coaxial, and 4, 6 and 8 ~~eight~~ conductor twisted pair media.

Please replace the third paragraph beginning on page no. 4 with the following paragraph:

Therefore, in the event that an enterprise resolves to wire a transmission network over an existing facility, typically the most expeditious and cost effective means is by routing a twisted pair CAT medium throughout the existing structure. Conversely, if an enterprise decides to install a surveillance network in an existing facility, the most expeditious and cost effective means is by routing a dedicated coaxial cable for the distribution system. This often results in three separate and independent wiring networks, comprised of three different transmission media, each employing a disparate transmission technology over virtually the same area of the facility. Still more paradoxically, each of the networks may be ported in essentially the same location **[[of]]** the facility for connecting to a specific device.

Please replace the first paragraph beginning on page no. 6 with the following paragraph:

The present invention is directed to a non-intrusive data transmission network for use in a healthcare facility and method for implementing such network. Each individual patient's room is equipped with a set-top control device ("SCD"), a separate camera, microphone, and control module, **[[and]]** camera control device ("CCD"). The SCD allows for a non-intrusive installation within a minimum amount of time. By utilizing the existing cable television infrastructure, the device creates a high-speed data network throughout the facility.

Please replace the first paragraph beginning on page no. 14 with the following paragraph:

Conversely, if the patient wishes to access the Internet through the HCF's cable system, the patient would then select the "Internet/Network" option on handheld remote control **130**. In that case, SW **120** routes RF signals from TV channel modulator **132** to the patient's television via output connection **122**. These RF signals are transformed from raw video and audio signals output from video circuitry **[[~~154~~ 153]]** and audio circuitry **155**, respectively, on motherboard **150**. Browser images displayed from video circuitry **154** originate from two primary sources, remotely from the HCF's intranet/Internet and locally from SCD **100** and the devices controlled locally by the SCD **100**. Therefore, in addition to providing television channels to the user, the HCF cable system should also support the movement of downstream data from remote data sources to SCD **100** and upstream from SCD **100** to remote data receptors.

Please replace the first paragraph beginning on page no. 24 with the following paragraph:

It should be understood that the underlying mechanism for supporting the video surveillance system is the use of the TCP/IP protocol suite for establishing and accessing video data generated at a specific nodal location on the network. Each device node on either existing cable distribution system **302** (DOCSIS supported node) or LAN **304** has a MAC address. These addresses are referenced to the physical location of the connection port in the HCF **~~that~~ in which** the device is coupled. Establishing a TCP/IP session with specific MAC address node is analogous to being connected to the corresponding physical site in the network and bringing up the real-time data being generated by a camera, microphones, *etc.* at that site. Network nodal sites or establishing a TCP/IP session with a MAC address at the node are password protected. With respect to patients' in the HCF, at check-in they will receive a URL (Uniform Resource Locator) address, room number, and a password for access data to be transmitted by the SCD in that room. Anyone knowing the URL address and

password will be able to navigate to the web page, and then log into the surveillance video data stream coming from that ~~**patient**~~ **patient's** room.

Please replace the second paragraph beginning on page no. 26 with the following paragraph:

Essentially, the central platform allows for multiple operations to co-exist on cable distribution system **302**, and also on LAN **304**. Internet based server **327** continually takes snapshots at each camera (location) and simultaneously stores them on hard disk drive **409**. The captured real-time video is accessible by anyone with the inherent rights and connection to network **302**, LAN **304** or an Internet connection. An exemplary authorization hierarchy proceeds as follows: public; patient; HCF staff level 3; HCF staff level 2; system administrator; site security; and HCF staff level 1, from least to most access authority. For example, certain real-time video views may be accessible to anyone from the HCF's home page, such as the front façade of the HCF building, a panoramic view of the HCF campus and/or scenic vistas taken from the HCF campus. These images are typically captured by one of the SCCs used by the HCF site security. At the next level, patients and visitors in public areas may be given access to images from certain cameras, such as commons, entrances, cafeterias and the like. Typically, these images are limited to the CSD in the patient's room, the nurses' station, SCCs located in common areas and those areas accessible to the public. The surveillance video generated in patient rooms is triple secured. Someone desiring to view video for a SCD in a patient room must know the URL address and room number for the patient's room and the current password before being authorized by server **327** to access the surveillance video stream from that room. The access authorization for the healthcare facility's staff is based on two criteria: their employment position/duties; and the physical location of their current work assignment. For example, level 3 staffers, such as nurses, technicians and specialists, need to be authorized to view images of only those patients under their care while the patients are located in their work assignment areas, such as the patient's room, treatment and rehabilitation areas, and ingress/egress to those

areas. Additionally, level 3 staffers have limited authority to view non-real-time image data from temporary storage **database 409**, but not from third-party storage **420**. Level 2 staffers, on the other hand, are higher level employees and privilege holders, such as doctors and medical specialists who give care to specific patients, regardless of the location of the patient's room in the HCF. Level 2 staffers have limited administrative authority to allow their staff members to view the video of their patients and may view real-time as well as non-real-time image data **on temporary storage database 409.** ~~**from on temporary storage 327.**~~ Additionally, certain level 2 staffers may have authorization codes for certain patient data on third-party storage **420**.

Please replace the first paragraph beginning on page no. 27 with the following paragraph:

It should be understood that privacy guidelines in an HCF are strictly regulated by rules promulgated under, for example, the Health Insurance Portability and Accountability Act (HIPPA). The capture, transmission, storage and access to patient data must comply with these privacy rules and may require that patient video data be encrypted and patients' identities substituted with unique identification codes prior to storage. In any case, certain HCF employees in non-healthcare employment positions may need a relatively high-level authorization in order to perform their duties, but still be denied access to the actual video images in all but the most extraordinary of circumstances. Thus, system administrators may have limited access to all data on network **302** and in **temporary** storage **409** and **third party storage 420**, but not their content. One means of ensuring that system administrators do not make unauthorized use of the surveillance system is to use filter masks and registries. For example, any video data ~~**access**~~ **accessed** by a system administrator may be checked for quality purposes in its raw form. However, a system administrator's view of patient images is strictly limited. These limitations include lowered image quality (*i.e.* resolution and size (under 72x36 dpi), short display durations (1-3 sec. maximum), read-only, non-archivable video). Each access is logged into a registry with the administrator's ID and other pertinent

information. Site security, the next level, is given authorization for viewing image data from any of the SCCs on the campus, as well as all authorization to operate pan, tilt and zoom features. Additionally, site security is given limited authorization to view unaltered images from any SCD in the HCF. Having an unobstructed view from any vantage point in the HCF is crucial for the safety of the occupants. For example, in case a fire alarm is triggered, the site security is given full access to any camera in any location in order to ensure that all occupants are accounted for. Police, fire and homeland security officials may also be given temporary authorization to use emergency keys, which may be either physical keys or logical password keys. The uppermost tier in the authorization hierarchy is reserved for HCF staff level 1 employees. This group of employees generally comprises high-level executives, administrators and overseers whose duties include reviewing and managing the patients as well as the HCF staff and contractors. Level 1 staffers have access to not only unaltered real-time and non-real-time images, but also to the registry logs associated with the identities of employees who have previously viewed the images. HCF staff level 1 employees are the oversight group which, as a whole, is responsible for scrutinizing patient care, as well as monitoring the conduct of other HCF employees.

Please replace the first paragraph beginning on page no. 30 with the following paragraph:

Screen **[[~~502~~ 500]]** is subdivided into two distinct frames: navigation frame **502** and image frame **504**. Navigation frame **502** is a graphical user interface (GUI) which depicts a graphic image of the physical layout of the HSF campus or a portion thereof. The user can scale and pan the graphic image and flip to adjacent or layered levels of the graphic using the pointing device. Landmarks are labeled on the graphic images as are "hotspots" with which the user may interact. These hotspots include iconic representations which identify the site locations of cameras in the HCF which the user is authorized to access, such as camera locations **506**. The locations of these hotspots on the graphic image change with the user's access authority. The video

image depicted in image frame **504** is a real-time image captured from one of camera locations **506** in which the user has authorization to view. The user can click around hotspots on graphic image **502** causing the video images in image frame **504** to change responsively. Additionally, the browser GUI allows the user to navigate to previously accessed camera locations using a "BACK" control on the interface and to a default camera location, predefined as the home camera location, using a "HOME" control adjacent to image frame **504** on the browser. Finally, image frame **504** may be scaled and/or maximized to cover the entire view window of the browser, thereby displacing navigation frame **502**. In either case, server **327** will update the picture every so often. The frame rate is dependent on a number of factors including the number of cameras used to connect to cable distribution system **302**, how much usage the primary control system needs at the time, and the user's access authority. The refresh frame rate can range from essentially live motion video (30 frames per second) to a new picture every several seconds.

Please replace the second paragraph beginning on page no. 32 with the following paragraph:

With regard to another aspect, image frames which have been identified as showing motion may be saved locally on drive **140** having several benefits. First, if the CMTS has not authorized the SCD to transmit or is temporarily allocating only a meager number **[[** ~~**og**~~ **of** **]]** upstream spaces, then the motion video data can be transmitted slightly time-delayed. Thus, if the motion captured by the camera is crucial, the data is locally backed up for safety purposes. This feature may also save video image data if the network goes down. Implementation may be performed in several variations. First, a motion detection area on the video frame may be selected. For instance, for addressing security concerns, only the difference outside the patient area might be considered between the two image frames. If differences as detected, that frame is flagged as having a higher priority, time stamped and temporarily saved locally on drive **140**. In order to conserve space on the drive, saved video frames will be overwritten,

but only after a predetermined time period has elapsed. Prior to that time, the flagged image frames are available to be downloaded or viewed on the television monitor in the patient's room. Alternatively, for addressing patient care concerns, only the differences detected between the two image frames in the patient area might be considered. Movement by healthcare professionals, family members and others who do not cross the path of the patient area will not trigger the image frame to be saved. In either case, the detection of slight motion will generally not cause the video to be saved. However, when the amount of change detected between the current frame and the last saved frames is above a threshold amount, the current frame is saved. These motion detection functions may be incorporated in camera **192**, video circuitry **153**, or may instead be implemented as a sub-routine of a software application. With this feature in place, it is possible to create a video history of the events occurring within the medical room, which is particularly useful in contrived lawsuits. By viewing the tapes, one can determine all aspects of the situation and in most cases where the true concern lies.

Please replace the second paragraph beginning on page no. 2 with the following paragraph:

Notice also that the healthcare ~~**processional**~~ **professional** can ~~**communicated**~~ **communicate** directly with any node on HCF's cable distribution system **302** or LAN **304**. For instance, should the healthcare ~~**processional**~~ **professional** desire to send a message back to her office computer in the HCF, the message is generated on wireless device **704**, passed to CSD **100** over wireless link **706** and onto bridge operation **712** over cable distribution system **302**. After the RF DOCSIS-based data is converted to the Ethernet data link protocol format, the message continues to server operations **714** and to Ethernet switch **718** for routing over LAN **304** to the healthcare professional's office computer **324**.

Please replace the first paragraph beginning on page no. 36 with the following paragraph:

Alternatively, the message recipient may be connected to LAN **304**. For instance, should the healthcare ~~**processional**~~ **professional** desire to send a message back to her office computer in the HCF, the generated data on wireless device **704** is passed to CSD **100** over wireless link **706** and onto bridge operation **712** over cable distribution system **302**. After the RF DOCSIS-based data is converted to the Ethernet data link protocol, the message continues on to server operations **714** and to Ethernet switch **718** for routing over LAN **304** to the healthcare professional's office computer **324**.

Please replace the second paragraph beginning on page no. 36 with the following paragraph:

In accordance with still another exemplary embodiment, implementation of the present invention on an existing cable distribution system enables a healthcare professional to enter a prescription, lab order or therapy request into the PC tablet and electronically transmit it ~~**electronically**~~ to the service provider. Using a prescription order as an example, the messaging process flows essentially as described above. The healthcare professional enters a prescription for medication on wireless data processor **704** which sends the data to SCD **100**, which places the message in the DOCSIS upstream data flow on network **302**. All upstream data is converted to Ethernet data link protocol by Ethernet to RF bridge process **712** and forwarded to server/software processes **714**. Here, the message address is checked against network routing tables and forwarded to the network having the pharmacy node address. It is expected that the pharmacy will be connected to LAN **304**, as will most other HCF service providers. However, server/software process **714** may route the message to either network (the existing DOCSIS enabled cable distribution system with or the Ethernet LAN) depending on the address. But typically, the message will be forwarded through one or more routers and/or switches **714** prior to reaching the pharmacy node. It is expected

that, upon receipt, the pharmacy device **708** will immediately respond to device **704** with a confirmation that the message has been received.

Please replace the second paragraph beginning on page no. 37 with the following paragraph:

In accordance with another exemplary embodiment of the present invention, doctors in non-LAN offices, such as office **804**, can see and speak with patients or families from anywhere in the hospital, even in other areas not supported by LAN **304**. These include patient rooms **802**, waiting rooms **806** and other doctors' offices, commons areas, conference rooms without Ethernet LAN connection. The process for creating and managing a video meeting is essentially similar to the process described above for data transmissions. For instance, a healthcare processional in office **804**, which does not have an Ethernet connection, desires a conference with a patient's family which is in a waiting room elsewhere in the HCF. Rather than traveling the length of the HCF, on occasion the professional may initiate a videoconference with the occupants of waiting room **806**. As discussed above, the professional interfaces with SCD **100B** using **[[a]]** wireless device, such as **[[a]]** keyboard and/or mouse **808B**, to initiate the conference request. SCD **100B** then sends the request to Ethernet to RF bridge operators **812** over existing cable distribution system **302** in a DOCSIS compliant form. The DOCSIS-based request is received by the Ethernet to RF bridge and forwarded to server/software operators **814** and **[[a an]]** Ethernet data link protocol message. Server/software operators **814** then locates recipient SCD **100C** and attempts to establish a video conference session. The session request is sent to Ethernet to RF bridge operators **816** (which is typically the same CMTS equipment that handled the doctors initiation request) and received by the CSD **100C** in waiting room **806**. The mechanisms for establishing video conferencing sessions are well known and will not be discussed in detail, but bi-directional data channel paths for video and audio (A/V)data are set up between SCD **100B** in office **804** and SCD **100C** in waiting room **806** for carrying A/V data in a near real-time manner.

Please replace the Abstract of the Disclosure beginning on page no. 46 with the following paragraph:

The present invention is directed to a non-intrusive data transmission network for use in a healthcare facility and method for implementing such network. Each individual patient's room is equipped with a set-top control device, a separate camera, microphone, **[[~~and~~]]** control module **[[, and]]** camera control device. The SCD allows for a non-intrusive installation within a minimum amount of time. By utilizing the existing cable television infrastructure, the device creates a high-speed data network throughout the facility. The interface **[[~~to~~]]** between the SCD and the CCD is accomplished through a standard interface for universally connecting auxiliary devices, such as USB, for enabling expandable, hot-pluggable Plug and Play serial device interfaces. These ports allow external devices such as the camera, microphone, infrared keyboard and privacy control unit to communicate with the SCD. Additional USB ports on the SCD allow for other devices to be connected to the network at a future time. Such devices include those for instrument monitoring, doctor information access or pharmaceutical prescription ordering. Visual information such as e-mail, web browsing, video and audio communications via web camera applications from family members, friends or other parties may be viewed by the patient from the in-room TV set by way of the internal RF modulator (and connecting to the Internet via the patient Internet server). The SCD switches from the standard cable TV channels to the SCD by way of an internal switch controlled by the patient from an infrared control. This control also enables or disables the camera to allow for privacy at times when such privacy is required from external Internet access. The system is configurable to offer this privacy to be layered from specific Internet or external users to the nurses, doctors or security department as the hospital desires.